Protasowicki, I., 2018, *Rola szkodliwego oprogramowania w geopolityce*,
Przegląd Geopolityczny, 26, s. 85-94.

Igor PROTASOWICKI
Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie

ROLA SZKODLIWEGO OPROGRAMOWANIA W GEOPOLITYCE

Abstrakt:

Ilość zagrożeń teleinformatycznych w świecie wzrasta dynamicznie wraz z upowszechnianiem wykorzystania systemów komputerowych w kolejnych obszarach ludzkiej aktywności. Współczesne państwa w znacznym stopniu zależne są od szybkiego dostępu do informacji uwzględniając także ich przechowywanie, przetwarzanie oraz przesyłanie, co sprawia, że obszar ten stał się elementem gry geopolitycznej. Społeczeństwa oraz powoływane przez nie organy i instytucje powszechnie wspomagają się rozwiązaniami komputerowymi. Obecnie komputer zaliczany jest do typowego wyposażenia gospodarstw domowych. Należy do tego doliczyć także skomputeryzowane urządzenia zaliczane do szeroko rozumianej elektroniki użytkowej. Analogicznie w sferze publicznej komputery i urządzenia skomputeryzowane stały się powszechne. Zagrożenia teleinformatyczne, takie jak szkodliwe oprogramowanie, w tym wirusy i robaki komputerowe, jak również ataki DoS/DDoS, kradzieże, podmiana i uszkadzanie danych jak również celowe uszkodzenia systemów komputerowych należy współcześnie zaliczyć do katalogu metod i środków rywalizacji w środowisku międzynarodowym. Właściwymi dla nauk społecznych, w tym nauk o bezpieczeństwie metodami analizy i krytyki literatury przedmiotu, metodą historyczną i metodą obserwacyjną dokonano selekcji oraz analizy wydarzeń świadczących o wykorzystaniu szkodliwego oprogramowania w geopolityce w przeszłości. Wskazano przykłady wykorzystania poszczególnych zagrożeń teleinformatycznych w rywalizacji międzynarodowej. Omówiono przebieg i skutki zastosowania szkodliwego oprogramowania, ataków DoS/DDoS oraz kradzieży danych wskazując współczesne metody i środki zabezpieczania przed omawianymi zagrożeniami. Określono także zakres i potencjalne znaczenie zagrożeń teleinformatycznych w geopolityce w przyszłości.

Słowa kluczowe: geopolityka, bezpieczeństwo, zagrożenie, komputer, wirus, robak, szkodliwe oprogramowanie, atak.

Wprowadzenie

Rola zagrożeń teleinformatycznych wzrasta wraz z rozpowszechnianiem się wykorzystania systemów teleinformatycznych. Pierwsze systemy komputerowe wspierały powoływane przez człowieka organizacje w najbardziej wymagających zadaniach obliczeniowych, jednak wraz z postępującą miniaturyzacją oraz rozwojem technologii sieciowych pojawiły się w niemal wszystkich obszarach naszej aktywności. Dynamicznie zwiększa się także zakres przedmiotowy danych i informacji przechowywanych, przetwarzanych i przesyłanych w systemach teleinformatycznych. Ta wszechobecność sieci komputerowych jako narzędzia ułatwiającego wymianę oraz przechowywanie informacji doprowadziła do sformułowania i wprowadzenia do powszechnego użytku pojęć takich jak „*big data*" oraz kategorii „*always online*".

Korzystając z dostępnych źródeł, właściwymi dla nauki o bezpieczeństwie metodami analizy i krytyki literatury przedmiotu oraz metodą obserwacyjną można jednoznacznie określić poziom wpływu, jaki zagrożenia teleinformatyczne wywierają na procesy geopolityczne. Dostępna literatura przedmiotu, zarówno z obszaru geopolityki, bezpieczeństwa narodowego i wewnętrznego jak i informatyki kompetentnie pokrywa ten obszar. Wnioski można uzupełnić obserwacjami zarówno historycznych, jak i bieżących wydarzeń.

Rodzaje zagrożeń

Do najpowszechniej występujących zagrożeń wobec systemów komputerowych zalicza się przede wszystkim:

1) szkodliwe oprogramowanie, w tym zwłaszcza robaki i wirusy komputerowe działające na zasadzie bomb logicznych, koni trojańskich itp., których głównym skutkiem jest destabilizacja działania systemów komputerowych, kradzież, uszkodzenie lub podmiana przechowywanych, przetwarzanych lub przesyłanych w nich danych;
2) chipping, czyli specjalne modyfikowanie urządzeń peryferyjnych w celu wykradania danych z systemów, do których zostaną one podłączone;
3) spoofing będący kradzieżą tożsamości innych użytkowników sieci komputerowej w celu podszywania się pod nich;
4) sniffing polegający na przechwytywaniu pakietów danych przesyłanych między urządzeniami podłączonymi do tej samej sieci;
5) flooding i spamming, których skutkiem jest zapełnianie pamięci masowej atakowanych systemów, oraz celowe niszczenie sprzętu komputerowego na przykład generatorami pola elektromagnetycznego (Protasowicki 2010, s. 129-130).

Rola zagrożeń teleinformatycznych we współczesnych konfliktach

Do powszechnego użytku wprowadzono także pojęcie „*wojny hybrydowej*", będącej rodzajem konfliktu, w którym strony wykorzystują jednocześnie metody i środki walki konwencjonalnej i niekonwencjonalnej, zagrożenia asymetryczne oraz metody walki elektronicznej i informacyjnej, wliczając w to dezinformację, agresywną dyplomację i ingerowanie w sprawy wewnętrzne innych państw (Fleming 2011, s. 2-3; Wasiuta 2016). W tym przypadku należy zwrócić uwagę na szczególną rolę, jaką wspomniane zagrożenia teleinformatyczne mogą odegrać.

Na przełomie XX i XXI wieku państwa z grupy wysokorozwiniętych dokładały starań, by konflikty zbrojne odsunąć jak najdalej od swoich granic. Prowadzenie działań zbrojnych wiąże się ze znaczącymi stratami ludnościowymi i ekonomicznymi, dlatego też współcześnie w pierwszej kolejności wykorzystuje się mechanizmy rozładowywania konfliktów i rozwiązywania sporów w miejscu ich powstania, zanim zdążą się one rozprzestrzenić terytorialnie. Z drugiej jednak strony lokalne konflikty są wykorzystywane przez mocarstwa globalne i regionalne do osiągania celów polityki wewnętrznej. Bezpośrednie lub pośrednie zaangażowanie militarne w takim konflikcie wiąże się z określonymi kosztami obciążającymi budżet wewnętrzny jak również determinuje inne procesy mogące destabilizować sytuację międzynarodową, jak migracja uchodźców itp. Do bezpośrednich starć między państwami wysoko rozwiniętymi dochodzi w innych obszarach – zwłaszcza w obszarze gospodarczym oraz z wykorzystaniem środków komunikacji elektronicznej.

Wykorzystanie zagrożeń komputerowych w geopolityce nie jest nowym zjawiskiem. Pierwsze informacje o wykorzystaniu szkodliwego oprogramowania w działaniach geopolitycznych sięgają okresu *zimnej wojny* i do dziś stanowią przedmiot sporu. W 1982 roku doszło do poważnej awarii zakończonej eksplozją gazociągu transsyberyjskiego. Wiele źródeł wskazuje, że był to efekt działalności sabotażowej ze strony amerykańskiej Centralnej Agencji Wywiadowczej, która zaatakowała komputerowy system zarządzania przesyłu gazu[1], podczas, gdy inne zaprzeczają, wskazując, że przyczyną wybuchu była zwykła awaria[2]. To konkretne wydarzenie nie zostało jednak opisane w żadnym źródle naukowym ani też należycie udokumentowane, dlatego też współcześnie można traktować je bardziej w kategoriach ciekawostki naukowej. Systemy komputerowe nie były w owym okresie na tyle powszechne, nie istniała sieć o zasięgu globalnym, a inwestycje strategiczne na terytorium ZSRR prowadzone były z zachowaniem istotnych środków bezpieczeństwa i w tajemnicy przed obywatelami. Należy zatem przyjąć, że nie istniały dostateczne środki do

[1] Np. https://www.gizmocrazed.com/2010/09/top-7-worst-cyber-attacks-in-history/ (dostęp dnia: 25.06.2018); https://rconnon12.wordpress.com/2014/10/26/third/ (dostęp dnia: 25.06.2018).

[2] Zob. http://www.infosecisland.com/blogview/21566-The-Myth-of-the-CIA-and-the-Trans-Siberian-Pipeline-Explosion.html (dostęp dnia: 25.06.2018).

pozyskania wiarygodnych dowodów, a pojawiające się nazwiska agentów poszczególnych państw, czy też informacje o spreparowaniu przez USA dokumentacji technicznej rozwiązań i urządzeń (obciążonej istotnymi błędami mogącymi znacząco ograniczać sprawność lub wręcz sprawiać zagrożenie), która została następnie wykradziona przez ZSRR i wykorzystana podczas budowy systemu komputerowego zarządzania gazociągiem transsyberyjskim[3] traktować należy ze stosownym dystansem, choć do wybuchu naprawdę doszło.

Państwa dokładają wszelkich starań, by nie dało się jednoznacznie potwierdzić ani posiadania przez nie sił i środków służących do walki w cyberprzestrzeni ani też powiązać ich bezpośrednio z atakami. Jednak coraz trudniej jest zatajać działalność w internecie mając na uwadze fakt, że dostęp do informacji oraz transparentność systemu sprawowania władzy jest przedmiotem zainteresowania obywateli – nie tylko państw demokratycznych – oraz to, że zawiązują oni formalne i nieformalne organizacje mające na celu oddolne pilnowanie tych procesów wykorzystując w tym celu wszelkie dostępne metody i środki.

Wykorzystanie zagrożeń teleinformatycznych w geopolityce

Przykładami współczesnego wykorzystania zagrożenia teleinformatycznego w geopolityce, które nie umknęły uwadze obywateli, państw ani społeczności międzynarodowej mogą być ataki cybernetyczne *Titan Rain*, zmasowane działania wymierzone przeciwko Estonii oraz robak komputerowy *Stuxnet* (Świątkowska 2017).

Ataki cybernetyczne typu *Titan Rain*

Szacuje się, że za pierwsze z wymienionych działań odpowiada grupa hackerów o tej samej nazwie (*Titan Rain*) a początek operacji datuje się w zależności od źródeł na 2001 lub 2003 rok. Celem działania hackerów była kradzież danych i informacji z sieci komputerowych należących do agencji rządowych oraz podmiotów współpracujących z rządem Stanów Zjednoczonych (Shelmire 2008, s. 2). Atak został wykryty przez pracownika *Sandia National Laboratory* (SNL), który prowadził dochodzenie w sprawie włamań do systemów informatycznych firmy *Lockheed Martin* i wykrył, że wkrótce po tych atakach celem podobnych stało się także SNL. Źródło ataku zlokalizowano w chińskiej prowincji Guangdong, a do 2006 roku sprawcy wykradli dane z *U.S. Army Information Engineering Command*, *Defense Information Systems Agency*, *U.S. Army Space and Strategic Command*, *Army Aviation and Missile Command*, Departamentu Energetyki, Departamentu Bezpieczeństwa Krajowego, Departmentu Stanu, oraz Akademii Marynarki Wojennej jak również nawet 20 terabajtów utajnionych (ale nie wrażliwych) danych z Departamentu Obrony (tamże).

[3] Zob. http://www.dsalert.org/int-experts-opinion/cyber-warfare/508-cyber-war-and-the-siberian-pipeline-explosion (dostęp dnia: 25.06.2018).

Co ciekawe, za pierwszą nagłośnioną w świecie kradzież danych z systemu komputerowego odpowiada grupa nastolatków z Milwaukee, którzy w 1981 roku stworzyli grupę *The 414s*. Przeprowadzone przez nich ataki były bardziej dziełem przypadku, niż efektem posiadanych umiejętności, ponieważ udało im się odgadnąć hasła dostępu między innymi do Los Alamos National Laboratory, Sloan-Kettering Cancer Center, oraz Security Pacific Bank[4]. Oprócz dostępu do zastrzeżonych danych podczas jednego z włamań do systemu operatora telekomunikacyjnego prawdopodobnie w celu zatarcia śladów wcześniejszej działalności wykasowali oni dane billingowe (Franklin 1990, s. 35). Obecnie kluczowe systemy teleinformatyczne nie są połączone z siecią globalną, co minimalizuje ryzyko uzyskania dostępu do danych przez osoby nieupoważnione. Z drugiej strony do zabezpieczenia danych przechowywanych, przetwarzanych i przesyłanych w systemach połączonych z internetem stosuje się zaawansowane metody i techniki kontroli dostępu, uwzględniające takie zabezpieczenia, jak uwierzytelnianie wielopoziomowe czy też szyfrowanie kaskadowe.

Ataki DoS/DdoS przeciwko Estonii

Kolejny spośród wyżej wspomnianych ataków wymierzony był przeciwko Estonii, a jego kulminacja datuje się na 17 maja 2007 roku. Uznaje się, że miał miejsce w odpowiedzi na przeniesienie pomnika tzw. „Brązowego Żołnierza" upamiętniającego udział Armii Czerwonej w wyzwoleniu Tallina spod okupacji niemieckiej podczas II wojny światowej. Plany przeniesienia pomnika spotkały się z typową dla tego typu wydarzeń reakcją dyplomatyczną ze strony Federacji Rosyjskiej, natomiast zaraz po oficjalnym proteście, w nocy z 26 na 27 kwietnia doszło na ulicach Tallina do zamieszek prowokowanych przez rosyjską młodzież. Wkrótce później, 27 kwietnia 2007 roku doszło do zmasowanych ataków typu DDoS wymierzonych przeciwko estońskim sieciom teleinformatycznym[5], w wyniku których doszło do zakłócenia funkcjonowania systemów komputerowych należących do estońskiego parlamentu, administracji rządowej, instytucji samorządowych oraz instytucji finansowych działających na terytorium tego państwa (Yap 2009, s. 8). Zgodnie z ustaleniami władz w Tallinie działania te zainicjowane zostały na terytorium Federacji Rosyjskiej, natomiast przywrócenie sprawności sprzed ataków trwało blisko trzy tygodnie. Mając na uwadze, że Estonia w tym okresie była najbardziej zinformatyzowanym krajem w Europie, skutki gospodarcze i społeczne przedmiotowego ataku były tym dotkliwsze (Czosseck, Ottis, Talihärm 2011, s. 24-34).

Ataki tego typu zdarzają się bardzo często, ponieważ ich realizacja jest relatywnie prosta i tania. Ich autorzy wykorzystują luki i naturalną słabość

[4] P. Elmer-DeWitt, *The 414 Gang Strikes Again*, Time, 29 sierpnia 1983, s. 75.
[5] https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html (dostęp dnia: 25.06.2018).

infrastruktury sieciowej obciążając ją specjalnie wygenerowanym ruchem (Apiecionek 2017, s. 240). Współcześnie do przeprowadzenia ataku DoS/DDoS wykorzystuje się tzw. *zombie networks*, czyli sieci urządzeń, nad którymi przejęto kontrolę z wykorzystaniem szkodliwego oprogramowania. Na żądanie hackera znaczna ilość takich urządzeń jednocześnie wysyła zapytania sieciowe do atakowanych systemów powodując ich przeciążenie. Z uwagi na ilość aktywnych urządzeń oraz relatywnie niski poziom świadomości ich użytkowników budowa dużej sieci *zombie* jest stosunkowo łatwa, natomiast w sieci można znaleźć oferty odpłatnych ataków na konkretne cele. Nie dziwią zatem dane szacunkowe, według których w 2017 roku mogło dojść nawet do 200 ataków DoS/DDoS dziennie[6]. Przygotowanie infrastruktury sieciowej na wypadek ataków DoS/DDoS jest wykonalne, choć im więcej ruchu dana sieć ma obsługiwać, tym wyższe będą koszty związane z zabezpieczeniem. Wykorzystuje się w tym celu tzw. *load balancery*, czyli urządzenia sieciowe odpowiedzialne za zarządzanie ruchem sieciowym. Mogą one działać w sposób bierny kierując poszczególne zapytania po równo między poszczególne serwery, mogą też w czasie rzeczywistym filtrować ruch sieciowy pod względem podejrzanych zachowań, jednak tego typu rozwiązanie przeważnie ogranicza ogólną wydajność systemu oraz przepustowość sieci, dlatego też w dużych centrach obsługi danych można je stosować w ograniczonym zakresie.

Stuxnet

Ostatnie z wymienionych przykładowych zagrożeń dowodzi, że odpowiednie zabezpieczenie zasobów teleinformatycznych jest coraz większym wyzwaniem. Robak komputerowy o nazwie *Stuxnet* wykorzystał bowiem sieć globalną do rozprzestrzenienia się po sieciach lokalnych, w których poszukiwał sterowników logicznych. Nie był jednak typowym robakiem komputerowym, ponieważ miał także możliwość infekowania i przenoszenia się za pośrednictwem pamięci przenośnych podłączanych do zainfekowanych komputerów. Tym sposobem został nieświadomie wprowadzony na teren niepołączonej z internetem sieci wewnętrznej irańskiego ośrodka badań jądrowych w Natanz. Zgromadzone przez *Stuxnet* informacje umożliwiły jego autorom przygotowanie drugiej wersji, której celem było zakłócenie funkcjonowania sterowników logicznych kontrolujących pracę wirówek wykorzystywanych w procesie wzbogacania uranu (Protasowicki 2016, s. 141). Podobnie jak w pozostałych przypadkach nie można jednoznacznie określić autora ataku, niemniej jednak przyjmuje się, że inicjatorem stworzenia tego robaka były organizacje wywiadowcze Stanów Zjednoczonych lub Izraela. Zwłaszcza, że efektem działania *Stuxnet*-u było znaczące opóźnienie irańskiego programu atomowego.

[6] Global Threat Landscape NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report, s. 10.

Przypadek *Stuxnet* bardzo dobrze obrazuje jak znaczną ewolucję przeszło zagrożenie związane ze szkodliwym oprogramowaniem. Pierwszy robak komputerowy zaatakował przez poważne niedopatrzenie ze strony jego autora. Robert Tappan Morris w 1988 roku próbował stworzyć oprogramowanie, które miało na celu ochronę własności intelektualnej opracowań naukowych, zamiast tego powstał robak komputerowy, który rozprzestrzeniał się z wykorzystaniem sieci komputerowej i replikował na zainfekowanych komputerach. W krótkim czasie (niecałych 20 godzin) znalazł się na około 10% urządzeń podłączonych do ówczesnej sieci globalnej (ARPANET) zajmując ich zasoby systemowe i sprawiając, że stały się nieużywalne. Gdy tylko Morris zorientował się, że stracił kontrolę nad swoim programem stworzył i rozesłał do wszystkich zaatakowanych ośrodków inny program, który miał powstrzymać działanie robaka i przywrócić normalną funkcjonalność urządzeń, jednak w międzyczasie zainfekowanych zostało około 6 tysięcy maszyn, zaś straty z tytułu ich unieruchomienia oceniono na 10-100 milionów dolarów (Dressler 2007). Architektura tego robaka w porównaniu ze współczesnymi przykładami szkodliwego oprogramowania była bardzo prosta, rozsyłał się on z wykorzystaniem protokołów TCP i SMTP i dawał się bez problemu wykryć (Spafford, 1989, s. 7-8). Zarówno robaki jak i wirusy z tamtego okresu były wykrywalne metodą słownikową, polegającą na przeszukiwaniu zawartości plików oraz transmisji danych w poszukiwaniu fragmentów znanych przykładów szkodliwego oprogramowania. Współcześnie jednak z jednej strony danych przesyła i przetwarza się zdecydowanie więcej, natomiast kod szkodliwych programów może być wewnętrznie zaszyfrowany (jak w przypadku *Stuxnet*) co uniemożliwia jego wykrycie na podstawie słownika. W związku z tym obecnie wykorzystuje się metody heurystyczne, polegające na obserwowaniu danych wejściowych i wyjściowych przetwarzanych przez zainstalowane w systemie programy w poszukiwaniu odstępstw od zarejestrowanych norm i wzorców wyniki budzące podejrzenia obejmując kwarantanną.

Podsumowanie

Przytoczone przykłady jednoznacznie dowodzą, że działania wymierzone przeciwko systemom komputerowym państw stanowią istotny element procesów geopolitycznych. Celem współczesnych konfliktów międzynarodowych nie jest powiększanie swoich terytoriów, lecz budowanie i rozwijanie wpływu, przekładające się na ekspansję gospodarczą. Metody i środki zaangażowania przeciwnika w spór wykluczają bezpośrednie starcie zbrojne, ponieważ to prowadziłoby do bezpośredniego zagrożenia wewnętrznych czynników produkcji. Dlatego też współcześnie stosuje się niemilitarne metody umożliwiające osłabienie przeciwnika – w tym metody komputerowe.

Istotnym aspektem w gospodarkach państw wysoko rozwiniętych jest ich uzależnienie od informacji. Za poziom rozwoju technologicznego

odpowiada zdolność do innowacji, która jest jednoznacznie zależna od wiedzy. Skuteczne konkurowanie na globalnym rynku wymaga stworzenia przez państwo przestrzeni do jej rozwoju. W przypadku, gdy subiektywne lub obiektywne okoliczności utrudniają rozwój wewnętrzny państwa działające na ich terytorium przedsiębiorstwa starają się pozyskać technologie innymi metodami. Także w tym kontekście powszechne wykorzystanie systemów komputerowych oraz sieci globalnej może być z jednej strony narzędziem ułatwiającym funkcjonowanie, z drugiej zaś istotnym wyzwaniem w obszarze zapewnienia bezpieczeństwa swoich danych i informacji. Rywalizacja technologiczna niejednokrotnie wiąże się z koniecznością zabezpieczenia swojej własności intelektualnej zarówno przed krajową jak i zagraniczną konkurencją, natomiast zagrożenia takie jak *Titan Rain* dowodzą, że zagrożenie wycieku, utraty, podmiany lub zniszczenia danych jest realne i poważne.

Upowszechnienie pojęcia wojny hybrydowej oraz współcześnie obserwowane procesy potwierdzają jednoznacznie, że szkodliwe oprogramowanie stało się nie tylko środkiem osiągania celów przez organizacje i struktury państwowe tworzone przez społeczeństwa, lecz stały się także orężem w arsenale państw. Nie powinno się zatem zadawać pytania „czy dane państwo dysponuje cyber-formacją", lecz raczej powinno się dokonać regularnych inwestycji w najnowocześniejsze dostępne zabezpieczenia istotnych danych i informacji. Ponad wszystko należy jednak pamiętać o konieczności nie tylko regularnej lecz wręcz stałej, czynionej w czasie rzeczywistym rewizji już istniejących zabezpieczeń pod kontem ich skuteczności wobec nowych i potencjalnych zagrożeń. Jako że udział systemów komputerowych jest powszechny niemal w każdym obszarze ludzkiej aktywności zasadnym byłoby wręcz powołanie wyspecjalizowanych formacji krajowych i międzynarodowych i powierzenie im takich kompetencji.

Literatura

Apiecionek, Ł., 2017, *Fuzzy Observation of DDoS Attack* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor Witold Kosiński*, P. Prokopowicz i in. (eds.), Springer Open, Cham/Switzerland.

Czosseck, C., Ottis, R., Talihärm, A.M., 2011, *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*, International Journal of Cyber Warfare and Terrorism (IJCWT), nr 1(1).

Dressler, J., 2007, *United States v. Morris*, *Cases and Materials on Criminal Law*, Thomson/West, St. Paul, MN.

Fleming, B.P., 2011, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, U.S. Army School of Advanced Military Studies (SAMS), U.S. Army Command & General Staff College, Skrypt, Fort Leavenworth.

Franklin, P., 1990, *Profits of Deceit: Dispatches from the Front Lines of Fraud*, Cornerstone Heinemann, London.

Protasowicki, I., 2016, *Bezpieczeństwo teleinformatyczne krytycznej infrastruktury elektroenergetycznej* [w:] *Geopolityka współczesnego bezpieczeństwa energetycznego. Wybrane aspekty*, M. Ilnicki, Ł. Nowakowski, I. Protasowicki (red.), Warszawa.

Protasowicki, I., 2017, *Rola zagrożeń teleinformatycznych w bezpieczeństwie wewnętrznym państwa* [w:] *Wybrane aspekty bezpieczeństwa państwa w wymiarze zewnętrznym i wewnętrznym*, I. Oleksiewicz (red. nauk.), Warszawa.

Shelmire, A., 2008, *The Chinese Cyber Attacks formerly known as Titan Rain*, Information Warfare, nr 95.

Soroka, P., 2016, *Rola nowoczesnych technologii w wyścigu zbrojeń*, Przegląd Geopolityczny, 16, s. 77-86.

Spafford, E.H., 1989, *The Internet Worm Program: An Analysis*, ACM SIGCOMM Computer Communication Review, vol. 19 issue 1, New York.

Świątkowska, J., 2017, *Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem*, Przegląd Geopolityczny, 20, s. 162-177.

Wasiuta, O., 2016, *Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym*, Przegląd Geopolityczny, 17, s. 26-40.

Yap, G.T., 2009, *When is a Hack an Attack? A Sovereign State's Options if Attacked in Cyberspace: A Case Study of Estonia 2007*, Air Command and Staff College Air University, Maxwell Air Force Base.

The role of malware in geopolitics

The amount of IT threats in the world is growing dynamically with the spread of the use of computer systems in the subsequent areas of human activity. Modern countries depend on quick access to information, including its storage, processing and transmission, which makes this area an element of the geopolitical game. Societies, organisations and institutions commonly support themselves with computer solutions both in private life and in public space. Currently, the computer is included in typical household equipment. It should also be added to computerized devices classified as consumer electronics. Similarly, in the public sphere, computers and computerized devices have become commonplace. ICT threats, such as malware, including viruses and computer worms, as well as DoS / DDoS attacks, thefts, replacements and data corruption as well as deliberate damage to computer systems are nowadays considered to be part of catalog of methods and means of competition in the international environment. The selection and analysis of events demonstrating the use of malware in geopolitics in the past were appropriate for social sciences, including security studies, through methods of analysis and criticism of the literature of subject, historical method and observational method. The examples of the use of particular ICT threats in international competition are indicated. The course and effects of using malware, DoS / DDoS attacks and data theft

are discussed, indicating contemporary methods and means of protection against these threats. The scope and potential significance of teleinformatic threats in geopolitics in the future was also defined.

Key words: geopolitics, security, threat, computer, virus, worm, malware, attack.